Article 29.

Protective Provisions and Maintenance of Student Records.

§ 115C-400. School personnel to report child abuse.

Any person who has cause to suspect child abuse or neglect has a duty to report the case of the child to the Director of Social Services of the county, as provided in Article 3 of Chapter 7B of the General Statutes. (1981, c. 423, s. 1; 1998-202, s. 13(bb).)

§ 115C-401. School counseling inadmissible evidence.

Information given to a school counselor to enable him to render counseling services may be privileged as provided in G.S. 8-53.4. (1981, c. 423, s. 1.)

§ 115C-401.1. Prohibition on the disclosure of information about students.

(a) It is unlawful for a person who enters into a contract with a local board of education or its designee to sell any personally identifiable information that is obtained from a student as a result of the person's performance under the contract. This prohibition does not apply if the person obtains the prior written authorization of the student's parent or guardian. This authorization shall include the parent's or guardian's original signature. The person shall not solicit this authorization and signature through the school's personnel or equipment or on school grounds.

(b) The following definitions apply in this section:

(1) "Contract" means a contract for the provision of goods or services.

(2) "Personally identifiable information" means any information directly related to a student, including the student's name, birthdate, address, social security number, individual purchasing behavior or preferences, parents' names, telephone number, or any other information or identification number that would provide information about a specific student.

(3) "Sell" means sell or otherwise use for a business or marketing purpose.

(c) A violation of subsection (a) of this section shall be punished as a Class 2 misdemeanor, and when the defendant is an organization as defined in G.S. 15A-773(c) the fine shall be five thousand dollars ($5,000) for the first violation, ten thousand dollars ($10,000) for a second violation, and twenty-five thousand dollars ($25,000) for a third or subsequent violation.

(d) Nothing in this section shall preclude the enforcement of civil remedies as otherwise provided by law.

(e) Nothing in this section prohibits the identification and disclosure of directory information in compliance with federal law and local board of education policy or procedure. (2001-500, s. 1.)

§ 115C-401.2. Student online privacy protection.

(a) Definitions. – The following definitions apply in this section:

(1) Covered information. – Personally identifiable information or material in any media or format that is any of the following:

a. Created by or provided to an operator by a student, or the student's parent or legal guardian, in the course of the student's, parent's, or legal

guardian's use of the operator's site, service, or application for K-12 school purposes.

b. Created by or provided to an operator by an employee or agent of a K-12 school or local school administrative unit for K-12 school purposes.

c. Gathered by an operator through the operation of a site, service, or application for K-12 school purposes and personally identifies a student, including, but not limited to, the following:

1. Information in the student's educational record or electronic mail.
2. First and last name.
3. Home address.
4. Telephone number.
5. Electronic mail address.
6. Other information that allows physical or online contact.
7. Discipline records.
8. Test results.
9. Special education data.
10. Juvenile dependency records.
11. Grades.
12. Evaluations.
13. Criminal records.
14. Medical records.
15. Health records.
16. Social Security number.
17. Biometric information.
18. Disabilities.
19. Socioeconomic information.
20. Food purchases.
21. Political affiliations.
22. Religious information.
23. Text messages.
24. Documents.
25. Student identifiers.
26. Search activity.
27. Photos.
28. Voice recordings.
29. Geolocation information.

(2) Interactive computer service. – As defined in 47 U.S.C. § 230.

(3) K-12 school. – A charter school, a regional school, or a school that offers any of grades kindergarten to 12 operated by a local board of education.

(4) K-12 school purposes. – Purposes that are directed by or that customarily take place at the direction of a K-12 school, a teacher, a local board of education, or the State Board of Education, or aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration

between students, school personnel, or parents, or are for the use and benefit of the K-12 school.

(5) Local board of education. – A local board as defined in G.S. 115C-5(5), a regional school board of directors as defined in G.S. 115C-238.61(5), or a board of directors of a nonprofit corporation operating a charter as provided in G.S. 115C-218.15.

(6) Operator. – To the extent that it is operating in this capacity, the operator of an Internet Web site, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes. An operator does not include a K-12 school or local board of education that operates an Internet Web site, online service, online application, or mobile application for that K-12 school or local board of education's own K-12 school purposes.

(7) Subcontractor. – An entity providing a service to an operator under contract and on its behalf to further a K-12 school purpose.

(8) Targeted advertising. – Presenting an advertisement to a student where the advertisement is selected based on information obtained or inferred over time from that student's online behavior, usage of applications, or covered information. Targeted advertising does not include advertising to a student at an online location based upon that student's current visit to that location, or in response to that student's request for information or feedback, without the retention of that student's online activities or requests over time for the purpose of targeting subsequent ads.

(b) Prohibitions for Operators. – An operator shall not knowingly do any of the following:

(1) Engage in targeted advertising on the operator's site, service, or application, or target advertising on any other site, service, or application if the targeting of the advertising is based on any information, including covered information and persistent unique identifiers, that the operator has acquired because of the use of that operator's site, service, or application for K-12 school purposes.

(2) Use information, including persistent unique identifiers, created or gathered by the operator's site, service, or application, to amass a profile about a student except in furtherance of K-12 school purposes. As used in this subdivision, "amass a profile" does not include the collection and retention of account information that remains under the control of the student, the student's parent or guardian, or K-12 school.

(3) Sell or rent a student's information, including covered information. This subdivision does not apply to the purchase, merger, or other type of acquisition of an operator by another entity, if the operator or successor entity complies with this section regarding previously acquired student information, or to national assessment providers if the provider secures

the express written consent of the parent or student who is at least 13 years of age given in response to clear and conspicuous notice, solely to provide access to employment, educational scholarships or financial aid, and to postsecondary educational opportunities.

(4) Except as otherwise provided in subsection (d) of this section, disclose covered information unless the disclosure is made for the following purposes:

a. In furtherance of the K-12 school purpose of the site, service, or application, if the recipient of the covered information disclosed under this sub-subdivision does not further disclose the information unless done to allow or improve operability and functionality of the operator's site, service, or application.

b. To ensure legal and regulatory compliance or protect against liability.

c. To respond to or participate in the judicial process.

d. To protect the safety or integrity of users of the site or others or the security of the site, service, or application.

e. To a third party for a school, educational, or employment purpose requested by the student or the student's parent or guardian, provided that that information is required not to be used or further disclosed by the third party for any other purpose.

f. To a subcontractor, if the operator contractually prohibits the subcontractor from using any covered information for any purpose other than providing the contracted service to or on behalf of the operator, prohibits the subcontractor from disclosing any covered information provided by the operator with subsequent third parties, and requires the subcontractor to implement and maintain reasonable security procedures and practices. This sub-subdivision does not prohibit the operator's use of information for maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application.

(c) Requirements for Operators. – An operator shall do all of the following:

(1) Implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information and protect that covered information from unauthorized access, destruction, use, modification, or disclosure.

(2) Delete a student's covered information within 45 days if the K-12 school or local board of education requests deletion of covered information under the control of the K-12 school or local board of education, or the K-12 school or local board of education notifies the operator of completion of services with that operator, unless a student who is at least 13 years of age, a parent, or a guardian provides express written consent given in response to clear and conspicuous notice to the maintenance of the covered information.

(d) Permissible Use or Disclosure of Information. – An operator may use or disclose covered information of a student under the following circumstances:

(1) If other provisions of federal or State law require the operator to disclose the information and the operator complies with the requirements of federal and State law in protecting and disclosing that information.

(2) As long as no covered information is used for advertising or to amass a profile on the student for purposes other than K-12 school purposes, for legitimate research purposes as required by State or federal law and subject to the restrictions under applicable State and federal law or as allowed by State or federal law in furtherance of K-12 school purposes or postsecondary educational purposes.

(3) To a K-12 school, local school administrative unit, or the State Board of Education, for K-12 school purposes, as permitted by State or federal law.

(4) At the direction of a K-12 school, local school administrative unit, or the State Board of Education, for K-12 school purposes, as permitted by State or federal law.

(e) Permissible Operator Actions. – This section does not prohibit an operator from doing any of the following:

(1) Using covered information that is not associated with an identified student within the operator's site, service, or application or other sites, services, or applications owned by the operator to improve educational products.

(2) Using covered information that is not associated with an identified student to demonstrate the effectiveness of the operator's products or services, including in their marketing.

(3) Sharing covered information that is not associated with an identified student for the development and improvement of educational sites, services, or applications.

(4) Using recommendation engines to recommend to a student either of the following:

a. Additional content relating to an educational, other learning, or employment opportunity purpose within the operator's site, service, or application if the recommendation is not determined in whole or in part by payment or other consideration from a third party.

b. Additional services relating to an educational, other learning, or employment opportunity purpose within the operator's site, service, or application if the recommendation is not determined in whole or in part by payment or other consideration from a third party.

(5) Responding to a student's request for information or for feedback to help improve learning without the information or response being determined in whole or in part by payment or other consideration from a third party.

(6) Using a student's information, including covered information, solely to identify or display information on nonprofit institutions of higher education or scholarship providers to the student if the provider secures

the express written consent of the parent or student who is at least 13 years of age given in response to clear and conspicuous notice.

(f) Limitations. – This section does not do any of the following:

(1) Limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or under a court order.

(2) Limit the ability of an operator to use student data, including covered information, for adaptive learning or customized student learning purposes.

(3) Apply to general audience Internet Web sites, general audience online services, general audience online applications, or general audience mobile applications, even if login credentials created for an operator's site, service, or application may be used to access those general audience sites, services, or applications.

(4) Limit service providers from providing Internet connectivity to schools or students and their families.

(5) Prohibit an operator of an Internet Web site, online service, online application, or mobile application from marketing educational products directly to parents if the marketing did not result from the use of covered information obtained by the operator through the provision of services covered under this section.

(6) Impose a duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance with this section on those applications or software.

(7) Impose a duty upon a provider of an interactive computer service to review or enforce compliance with this section by third-party content providers.

(8) Prohibit students from downloading, exporting, transferring, saving, or maintaining their own student data or documents.

(g) A parent, K-12 school, teacher, local board of education, or the State Board of Education may report an alleged violation of this section to the Attorney General. The Attorney General, upon ascertaining that an operator has violated this section, may bring a civil action seeking injunctive and other equitable relief. Nothing in this section shall be construed to create a private right of action. (2016-11, s. 1; 2017-57, s. 7.26A.)

§ 115C-402. Student records; maintenance; contents; confidentiality.

(a) The official record of each student enrolled in North Carolina public schools shall be permanently maintained in the files of the appropriate school after the student graduates, or should have graduated, from high school unless the local board determines that such files may be filed in the central office or other location designated by the local board for that purpose.

(b) The official record shall contain, as a minimum, adequate identification data including date of birth, attendance data, grading and promotion data, and such other factual information as may be deemed appropriate by the local board of education having jurisdiction over the school wherein the record is maintained. Each student's official record also shall include notice of any long-term suspension or expulsion imposed pursuant to G.S. 115C-390.7 through G.S. 115C-390.11 and the conduct for which the student was suspended or expelled. The superintendent or the superintendent's designee shall expunge from the record the notice of suspension or expulsion if the following criteria are met:

(1) One of the following persons makes a request for expungement:
   a. The student's parent, legal guardian, or custodian.
   b. The student, if the student is at least 16 years old or is emancipated.

(2) The student either graduates from high school or is not expelled or suspended again during the two-year period commencing on the date of the student's return to school after the expulsion or suspension.

(3) The superintendent or the superintendent's designee determines that the maintenance of the record is no longer needed to maintain safe and orderly schools.

(4) The superintendent or the superintendent's designee determines that the maintenance of the record is no longer needed to adequately serve the child.

(c) Notwithstanding subdivision (b)(1) of this section, a superintendent or the superintendent's designee may expunge from a student's official record any notice of suspension or expulsion provided all other criteria under subsection (b) are met.

(d) Each local board's policy on student records shall include information on the procedure for expungement under subsection (b) of this section.

(e) The official record of each student is not a public record as the term "public record" is defined by G.S. 132-1. The official record shall not be subject to inspection and examination as authorized by G.S. 132-6.

(f) The actual address and telephone number of a student who is a participant in the Address Confidentiality Program established pursuant to Chapter 15C of the General Statutes or a student with a parent who is a participant in the Address Confidentiality Program established pursuant to Chapter 15C of the General Statutes shall be kept confidential from the public and shall not be disclosed except as provided in Chapter 15C of the General Statutes. (1975, c. 624, ss. 1, 2; 1981, c. 423, s. 1; 1985, c. 268; c. 416; 1997-443, s. 8.29(s); 2001-195, s. 1; 2002-171, s. 6; 2011-282, s. 13.)

§ 115C-402.2: Reserved for future codification purposes.

§ 115C-402.3: Reserved for future codification purposes.

§ 115C-402.4: Reserved for future codification purposes.

§ 115C-402.5. Student data system security.

(a) Definitions. – The following definitions apply in this section:

(1) Aggregate student data. – Data collected or reported at the group, cohort, or institutional level.

(2) De-identified student data. – A student dataset in which parent and student personal or indirect identifiers, including the unique student identifier, have been removed.

(3) FERPA. – The federal Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.

(4) Personally identifiable student data. – Student data that:

a. Includes, but is not limited to, the following:

1. Student name.
2. Name of the student's parent or other family members.
3. Address of the student or student's family.
4. Personal identifier, such as the student's Social Security number or unique student identifier.
5. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name.
6. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.
7. Information requested by a person who the Department of Public Instruction or local school administrative unit reasonably believes knows the identity of the student to whom the education record relates.

b. Does not include directory information that a local board of education has provided parents with notice of and an opportunity to opt out of disclosure of that information, as provided under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, unless a parent has elected to opt out of disclosure of the directory information.

(5) Student data system. – The student information management system used by the State Board of Education and Department of Public Instruction as part of the Uniform Education Reporting Systems for collection and reporting of student data from local boards of education.

(b) Security of Student Data System. – To ensure student data accessibility, transparency, and accountability relating to the student data system, the State Board of Education shall do all of the following:

(1) Create and make publicly available a data inventory and index of data elements with definitions of individual student data fields in the student data system, including, but not limited to:

a. Any personally identifiable student data required to be reported by State and federal education mandates.

b. Any other individual student data which has been proposed for inclusion in the student data system, with a statement regarding the purpose or reason for the proposed collection.

(2) Develop rules to comply with all relevant State and federal privacy laws and policies that apply to personally identifiable student data in the student data system, including, but not limited to, FERPA and other relevant privacy laws and policies. At a minimum, the rules shall include the following:

a. Restrictions on access to personally identifiable student data in the student data system to the following individuals:

1. Authorized staff of the State Board of Education and Department of Public Instruction and the contractors working on behalf of the Department who require such access to perform their assigned duties.
2. Authorized North Carolina public school administrators, teachers, and other school personnel and contractors working on behalf of the board of the North Carolina public school who require such access to perform their assigned duties.
3. Students and their parents or legal guardians, or any individual that a parent or legal guardian has authorized to receive personally identifiable student data.
4. Authorized staff of other State agencies and contractors working on behalf of those State agencies as required by law and governed by interagency data-sharing agreements.

b. Criteria for approval of research and data requests for personally identifiable student data in the student data system made to the State Board of Education from State or local agencies, researchers working on behalf of the Department, and the public.

(3) Prohibit the transfer of personally identifiable student data in the student data system to individuals other than those identified in subdivision (2) of this subsection, unless otherwise permitted by law and authorized by rules adopted under this section. Such rules shall authorize the release of personally identifiable data out of State to schools or educational agencies when a student enrolls in a school out of State or a local school administrative unit seeks help with locating a student formerly enrolled in this State who is now enrolled out of State.

(4) Develop a detailed data security plan for the student data system that includes all of the following:

a. Guidelines for authorizing access to the student data system and to individual student data, including guidelines for authentication of authorized access.
b. Privacy compliance standards.
c. Privacy and security audits.
d. Breach planning, notification, and procedures.
e. Data retention and disposition policies.

f. Data security policies, including electronic, physical, and administrative safeguards such as data encryption and training of employees.

(5) Ensure routine and ongoing compliance by the Department of Public Instruction with FERPA, other relevant privacy laws and policies, and the privacy and security rules, policies, and procedures developed under the authority of this section related to personally identifiable student data in the student data system, including the performance of compliance audits within the Department.

(6) Ensure that any contracts for the student data system that include de-identified student data or personally identifiable student data and are outsourced to private contractors include express provisions that safeguard privacy and security and include penalties for noncompliance.

(7) Notify the Governor and the General Assembly annually by October 1 of the following:

a. New student data, whether aggregate data, de-identified data, or personally identifiable student data, included or proposed for inclusion in the student data system for the current school year.

b. Changes to existing data collections for the student data system required for any reason, including changes to federal reporting requirements made by the United States Department of Education.

(c) Restricting on Student Data Collection. – The following information about a student or a student's family shall not be collected in nor reported as part of the student data system:

(1) Biometric information.

(2) Political affiliation.

(3) Religion.

(4) Voting history. (2014-50, s. 1.)

§ 115C-402.6: Reserved for future codification purposes.

§ 115C-402.7: Reserved for future codification purposes.

§ 115C-402.8: Reserved for future codification purposes.

§ 115C-402.9: Reserved for future codification purposes.

§ 115C-402.10: Reserved for future codification purposes.

§ 115C-402.11: Reserved for future codification purposes.

§ 115C-402.12: Reserved for future codification purposes.

§ 115C-402.13: Reserved for future codification purposes.

§ 115C-402.14: Reserved for future codification purposes.

§ 115C-402.15. Parental notification regarding rights to student records and opt-out opportunities.

(a) Annual Parental Notification. – Local boards of education shall annually provide parents, by a method reasonably designed to provide actual notice, information on parental rights under State and federal law with regards to student records and opt-out opportunities for disclosure of directory information as provided under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and notice and opt-out opportunities for surveys covered by the Protection of Pupil Rights Amendment, 20 U.S.C. § 1232h.

(b) Notice Content. – The notice shall include information on parental rights under State and federal law to:

(1) Inspect and review education records.

(2) Seek to amend inaccurate education records.

(3) Provide written consent prior to disclosure of personally identifiable information from education records, except as otherwise provided by law. Information shall be included on disclosure of directory information and parental rights to opt out of disclosure of directory information.

(4) File a complaint with the U.S. Department of Education concerning alleged failures to comply with the Family Educational Rights and Privacy Act.

(5) Receive notice and the opportunity to opt out prior to the participation of the student in a protected information survey under 20 U.S.C. § 1232h. (2014-50, s. 2.)

§ 115C-403. Flagging and verification of student records; notification of law enforcement agencies.

(a) Upon notification by a law enforcement agency or the North Carolina Center for Missing Persons of a child's disappearance, the superintendent of a local school administrative unit or his designee shall flag or mark the record of any child who is currently or was previously enrolled in a school of that unit and who is reported as missing. The flag or mark shall be made in such a manner that when a copy of or information regarding the record is requested, school personnel are alerted to the fact that the record is that of a missing child.

Before providing a copy of the school record or other information concerning the child whose record is flagged pursuant to this section, the superintendent or his designee shall notify the agency that requested that the record be flagged of every inquiry made concerning the flagged record, and shall provide a copy to the agency of any written request for information concerning the flagged record.

(b) When any child transfers from one school system to another school system, the receiving school shall, within 30 days of the child's enrollment, obtain the child's record from the school from which the child is transferring. If the child's parent, custodian, or guardian provides a copy of the child's record from the school from which the child is transferring, the receiving school shall, within 30 days of the child's enrollment, request written verification of the school record by contacting the school or institution named on the transferring child's record. Upon receipt of a request, the principal or the principal's designee of the school from which the child is transferring shall not withhold the record or verification for any reason, except as is authorized under the Family Educational Rights and Privacy Act. Any information received indicating that the transferring child is a missing child shall be reported to the North Carolina Center for Missing Persons. (1989, c. 331, s. 1; 1998-220, s. 12.)

§ 115C-404. Use of juvenile court information.

(a) **(Effective until December 1, 2019)** Written notifications received in accordance with G.S. 7B-3101 and information gained from examination of juvenile records in accordance with G.S. 7B-3100 are confidential records, are not public records as defined under G.S. 132-1, and shall not be made part of the student's official record under G.S. 115C-402. Immediately upon receipt, the principal shall maintain these documents in a safe, locked record storage that is separate from the student's other school records. The principal shall shred, burn, or otherwise destroy documents received in accordance with G.S. 7B-3100 to protect the confidentiality of the information when the principal receives notification that the court dismissed the petition under G.S. 7B-2411, the court transferred jurisdiction over the student to superior court under G.S. 7B-2200, or the court granted the student's petition for expunction of the records. The principal shall shred, burn, or otherwise destroy all information gained from examination of juvenile records in accordance with G.S. 7B-3100 when the principal finds that the school no longer needs the information to protect the safety of or to improve the educational opportunities for the student or others. In no case shall the principal make a copy of these documents.

(a) **(Effective December 1, 2019)** Written notifications received in accordance with G.S. 7B-3101 and information gained from examination of juvenile records in accordance with G.S. 7B-3100 are confidential records, are not public records as defined under G.S. 132-1, and shall not be made part of the student's official record under G.S. 115C-402. Immediately upon receipt, the principal shall maintain these documents in a safe, locked record storage that is separate from the student's other school records. The principal shall shred, burn, or otherwise destroy documents received in accordance with G.S. 7B-3100 to protect the confidentiality of the information when the principal receives notification that the court dismissed the petition under G.S. 7B-2411, the court transferred jurisdiction over the student to superior court under G.S. 7B-2200.5 or G.S. 7B-2200, or the court granted the student's petition for expunction of the records. The principal shall shred, burn, or otherwise destroy all information gained from examination of juvenile records in accordance with G.S. 7B-3100 when the principal finds that the school no longer needs the information to protect the safety of or to improve the educational opportunities for the student or others. In no case shall the principal make a copy of these documents.

(b) Documents received under this section shall be used only to protect the safety of or to improve the education opportunities for the student or others. Information gained in accordance with G.S. 7B-3100 shall not be the sole basis for a decision to suspend or expel a student. Upon receipt of each document, the principal shall share the document with those individuals who have (i) direct guidance, teaching, or supervisory responsibility for the student, and (ii) a specific need to know in order to protect the safety of the student or others. Those individuals shall indicate in writing that they have read the document and that they agree to maintain its confidentiality. Failure to maintain the confidentiality of these documents as required by this section is grounds for the dismissal of an employee who is not employed on contract, grounds for dismissal of an employee on contract in accordance with G.S. 115C-325.4(a)(9), and grounds for dismissal of an employee who is a career employee in accordance with G.S. 115C-325(e)(1)i.

(c) If the student graduates, withdraws from school, is suspended for the remainder of the school year, is expelled, or transfers to another school, the principal shall return all documents not destroyed in accordance with subsection (a) of this section to the juvenile court counselor and, if applicable, shall provide the counselor with the name and address of the school to which the student is transferring. (1997-443, s. 8.29(f); 1998-202, ss. 8, 13(cc); 1998-217, s. 12; 2000-140, s. 25; 2013-360, s. 9.7(l), (v); 2017-57, s. 16D.4(q); 2017-157, ss. 2(i), (n).)

§ 115C-405. Reserved for future codification purposes.

§ 115C-406. Reserved for future codification purposes.